

REMARKS

Claims 1-23 are pending in the application. Claim 23 is newly added. Reconsideration of this application is respectfully requested.

The Office Action rejects claims 1, 2, 5, 9, 10, 12, 16-19 and 21 under 35 U.S.C. 102(e) as anticipated by U.S. Patent No. 6,502,135 to Munger et al., hereafter Munger.

This rejection is traversed because Munger lacks each of the steps/elements recited in independent claims 1, 9 and 16.

In the Response to Non-final Office Action filed on April 27, 2006, Applicant set forth detailed arguments as to why independent claims 1, 9 and 16 are not anticipated by Munger. In paragraph 4 of the Office Action, the Examiner "respectfully disagreed" with Applicant's arguments, but did not specify what elements and steps in Munger are pertinent. It would be helpful if the Examiner would specifically identify which elements in Munger correspond to the victim machine v, the router r immediately upstream of v and the neighbor n, which are recited in independent claims 1, 9 and 16.

The claimed invention is a method (independent claims 1 and 16) and a backtracking unit (independent claim 9) for tracing a denial-of-service attack on a victim machine back towards its source.

In contrast, Munger discloses a system for secure communication between an initiating TARP terminal 100 and a destination TARP terminal 110. The system employs specific schemes for avoiding attempts of an eavesdropper to monitor network traffic. Munger uses a router hopping scheme in which each router in the message propagation path determines with a random number generator the next hop in a series of hops. See Fig. 2 and columns 7 and 8.

Munger also discloses a special address scheme to provide security from those who want to analyze the web traffic of initiating terminal 100. See column 11, line 44, to column 12, line 25. The Examiner refers to this citation as support for the contention that Munger shows the operation of a traceback program step/element recited in independent claims 1, 9 and 16. Independent claims 1 and 9 recite the operation of a traceback program to receive two input parameters, the IP address (v) of the victim machine and the IP address (r) of a router that is immediately upstream of the victim machine. However, this citation discloses an avoidance of an attack, which is not a traceback program to determine the source of the attack. This citation also discloses that Munger's TARP terminals and routers change IP addresses in response to an attack (column 11, lines 52 and 53). This response is merely an avoidance and in no way constitutes the operation of a traceback program. This response is not disclosed as determining IP addresses for the victim machine and a router immediately upstream of the victim machine.

This citation further discloses that the TARP process may also create a subprocess that maintains the original IP address and continues interacting with the attacker. The interaction may provide an opportunity to trace the attacker or study the attacker's methods. (column 12, lines 9-19). However, there is no disclosure or teaching that the subprocess in anyway receives the IP addresses v and r of the victim machine and a router immediately upstream of the victim machine. In fact, there is no disclosure of the specifics of how "interacting with the attacker" provides "an opportunity to trace the attacker". Moreover, there is no indication that the attack is "denial of service attack" as recited in independent claims 1, 9 and 16. Therefore, Munger does not disclose or teach a traceback program.

Independent claims 1 and 9 further recite the determination of a set of routers that are neighbors of r. The Examiner contends that Munger discloses this determination, citing column 16, lines 16-55. However, this citation discloses

a synchronization scheme for establishing a secure session between a client terminal 801 or 901 and a TARP router 811 or 911. There is no disclosure that TARP router 811 or 911 or the relationship of router 811 or 911 with another router that satisfies the relationship of a router *n* and a router that has an IP address *r* and that is immediately upstream of the victim machine as claimed. Moreover, this citation does not disclose the determination of a set of routers that are neighbors (*n*) of router *r*. Without the Examiner's identification of Munger's *v*, *r*, and *n*, it is impossible to know how the Examiner is analyzing Munger vis-à-vis independent claims 1, 9 and 16.

Independent claims 1 and 9 further recite:

"for each neighbor *n* of *r*, determining if *r* is *n*'s next-hop for traffic addressed to *v*, or to a network that *v* is on, where node *n*'s next-hop for traffic addressed to *v* is the IP address of the node that *n* will forward a packet to if the destination address in the packet is *v*".

The Examiner contends that Munger discloses this determination, citing column 16, line 56 to column 18, line 28. Column 16, line 56 to column 17, line 29 continues the client terminal 801 and TARP router 811 or client terminal 901 and TARP router 911 session. As discussed above, this session does not involve TARP router 811 or 911 or the relationship of router 811 or 911 with another router that satisfies the relationship of a router *n* and a router that has an IP address *r* and that is immediately upstream of the victim machine as claimed. Moreover, this citation does not disclose the determination of "if *r* is *n*'s next-hop for traffic addressed to *v*, or to a network that *v* is on, where node *n*'s next-hop for traffic addressed to *v* is the IP address of the node that *n* will forward a packet to if the destination address in the packet is *v*".

Column 17, line 30, to column 18, line 14, discloses a TARP node that includes an Ethernet local network. There is no disclosure of the claimed determination involving n , r and v (the victim machine's IP address).

Column 18, lines 15-28, describe an extension in which a client (801 or 911) uses multiple physical paths in order to provide link redundancy and further thwart attempts at denial of service and traffic monitoring. This involves three simultaneous sessions with each of three different TARP routers, where the physical paths are three different telephone lines. Again, there is no disclosure of the claimed determination for each neighbor n of the router r that is immediately upstream of the victim machine.

Independent claims 1 and 9 further recite:

"if r is not n 's next-hop for traffic addressed to v , skip over n and query the next neighbor of r , while if r is n 's next-hop for traffic addressed to v , determining an amount of traffic that n is forwarding to r that is addressed to v ".

The Examiner contends that Munger discloses the recited skip over n and determination of an amount of traffic step, again citing column 16, line 56 to column 18, line 28. Again, there has been no identification as to which of Munger's elements correspond to v , r and n . Moreover, the citation does not disclose or teach the determination of "an amount of traffic that n is forwarding to r that is addressed to v ", as recited in independent claims 1 and 9.

Independent claims 1 and 9 further recite:

"after determining the identity of the neighbor n of r that is the principal source of packets flowing to r that are addressed to v , continuing one node further upstream from the determined neighbor n of r that is the

principal source of packets flowing to r that are addressed to v, and continuing to traceback through interconnected routers until a source of denial-of-service attack packets to v is determined or until further traceback is not possible”.

The Examiner contends that Munger discloses the recited continuation of the traceback through interconnected routers, again citing column 16, line 56 to column 18, line 28. Again, there has been no identification as to which of Munger’s elements correspond to v, r and n. Moreover, this citation does not disclose or teach (1) continuing the traceback one node further upstream and (2) continuing to traceback through interconnected routers “until a source of denial-of-service attack packets to v is determined or until further traceback is not possible”. As discussed above, Munger does not teach a traceback program. Moreover, Munger does not mention “denial-of-service attack packets” or tracing back through interconnected routers to find a source of such packets.

Therefore, Munger lacks each of the steps/elements of independent claims 1 and 9 for the reasons set forth above.

The Examiner’s discussion of claim 16 treats independent claim 16 as reciting the same steps as independent claim 1. However, independent claim 16 has entirely different language. Therefore, the Examiner’s treatment of claim 16 is erroneous.

Based on the above discussion of the Examiner’s citations, it is noted that Munger does not disclose or teach any of the steps recited in independent claim 16, operating a traceback function, determining a set of network routers that are neighbors n of a network router r, querying individual ones of packet routers addressed to v via r and continuing to query packet routers up through a hierarchy of interconnected packet routers until an identity of the source is discovered or until further backtracking is impossible.

For the reason set forth above, it is submitted that the rejection of claims 1, 2, 5, 9, 10, 12, 16-19 and 21 under 35 U.S.C. 102(e) as anticipated by Munger is erroneous and should be withdrawn.

The Office Action rejects claims 3, 4 and 11 under 35 U.S.C 103(a) as unpatentable over Munger as applied to claims 1 and 9, and further in view of U.S. Patent No. 6,535,507 to Li et al., hereafter Li.

This rejection is erroneous for the reason that Munger lacks each of the steps/elements of independent claims 1 and 9, from which claims 3, 4 and 11 depend. Li, which was cited for a different reason, does not disclose this deficiency of Munger.

For the reasons set forth above, it is submitted that the rejection of claims 3, 4 and 11 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claims 6 and 13 under 35 U.S.C 103(a) as unpatentable over Munger as applied to claims 1 and 9, and further in view of U.S. Patent No. 5,963,540 to Bhaskaran, hereafter Bhaskaran.

This rejection is erroneous for the reason that Munger lacks each of the steps/elements of independent claims 1 and 9, from which claims 6 and 13 depend. Bhaskaran, which was cited for a different reason, does not disclose this deficiency of Munger.

For the reasons set forth above, it is submitted that the rejection of claims 6 and 13 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claims 7 and 14 under 35 U.S.C 103(a) as unpatentable over Munger as applied to claims 1 and 9, and further in view of U.S. Patent No. 6,636,509 to Hughes, hereafter Hughes.

This rejection is erroneous for the reason that Munger lacks each of the steps/elements of independent claims 1 and 9, from which claims 7 and 14 depend. Hughes, which was cited for a different reason, does not disclose this deficiency of Munger.

For the reasons set forth above, it is submitted that the rejection of claims 7 and 14 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claims 8 and 15 under 35 U.S.C 103(a) as unpatentable over Munger as applied to claims 1 and 9, and further in view of U.S. Patent No. 6,298,041 to Packer, hereafter Packer.

This rejection is erroneous for the reason that Munger lacks each of the steps/elements of independent claims 1 and 9, from which claims 8 and 15 depend. Packer, which was cited for a different reason, does not disclose this deficiency of Munger.

For the reasons set forth above, it is submitted that the rejection of claims 8 and 15 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claim 20 under 35 U.S.C 103(a) as unpatentable over Munger as applied to claim 16, and further in view of U.S. Patent No. 6,456,597 to Bare, hereafter Bare.

This rejection is erroneous for the reason that Munger lacks each of the steps/elements of independent claim 16, from which claim 20 depends. Bare,

which was cited for a different reason, does not disclose this deficiency of Munger.

For the reasons set forth above, it is submitted that the rejection of claim 20 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claim 22 under 35 U.S.C 103(a) as unpatentable over Munger in view of U.S. Patent No. 6,502,135 to Bhaskaran, hereafter Bhaskaran.

Independent claim 22 recites:

“operating a traceback program on at least one path to receive two input parameters, (a) an IP address (v) of the victim machine and (b) an IP address (r) of a router that is immediately upstream of the victim machine”.

The Examiner contends that this recited feature is disclosed by Munger, citing column 13, lines 30-43. This citation does not teach a traceback program, but rather a program or procedure for inserting and propagating decoy Tarp packets “to foil traffic analysis efforts” (column 12, line 24). This citation describes steps S9, S10 and S11 of Fig. 5 in which steps S9-S11 prepare a Tarp packet for propagation to the next hop router or to the destination (if the TTL counter has expired). There is no victim machine of a denial of service of attack. Munger merely propagates a Tarp packet to a next hop router.

Independent claim 22 further recites “determining a set of routers that are neighbors (n) of r”. The Examiner contends that Munger discloses this step, citing column 16, line 66 to column 17, line 31. However, this citation describes transmit and receive tables of IP addresses that are used by a pair of Tarp routers engaged in the propagation of a Tarp packet. The tables are used to change the IP addresses of each router for the propagation of the Tarp packet to

foil an eavesdropper's attempts to gain access to the Tarp packets. Munger calls this address changing scheme "IP hopping". There are only two Tarp routers involved in this citation. There is no determination of a set of routers that are neighbors (n) of r.

Independent claim 22 further recites:

"for each neighbor n of r, determining if r is n's next-hop for traffic addressed to v, or to a network that v is on, where node n's next-hop for traffic addressed to v is the IP address of the node that n will forward a packet to if the destination address in the packet is v".

The Examiner contends that this feature is disclosed by Munger, citing column 17, lines 32-51. This citation deals with the propagation of Tarp packets in the network using the IP-hopping scheme and within an Ethernet using fixed addresses. There is no victim machine of a denial of service of attack and, therefore, no router r or neighbor (n). Munger merely propagates a Tarp packet to a next hop router.

Independent claim 22 further recites:

"if r is not n's next-hop for traffic addressed to v, skip over n and query the next neighbor of r, while if r is n's next-hop for traffic addressed to v, determining an amount of traffic that n is forwarding to r that is addressed to v by sending at least one message to a neighbor router n for determining a count of packets that router n is sending to router r that are addressed to v or to a network on which v resides".

The Examiner contends that this feature is disclosed by Munger, citing column 17, lines 32-51. This citation deals with the propagation of Tarp packets in the network using IP-hopping scheme and within an Ethernet using fixed

addresses. There is no victim machine of a denial of service of attack and, therefore, no router r or neighbor (n). There is no determination of an amount of traffic or of a count of packets that n is sending to r. Munger merely propagates a Tarp packet to a next hop router.

Independent claim 22 further recites:

“after determining the identity of the neighbor n of r that is the principal source of packets flowing to r that are addressed to v, continuing one node further upstream from the determined neighbor n of r that is the principal source of packets flowing to r that are addressed to v, and continuing to traceback through interconnected routers until a source of denial-of-service attack packets to v is determined or until further traceback is not possible”.

The Examiner contends that this feature is disclosed by Munger, citing column 17, lines 52-67. However, this citation merely continues the description of the propagation of Tarp packets in the network using the IP-hopping scheme and within an Ethernet using fixed addresses. The citation also describes a node at the border of the Ethernet and The Tarp network generates a range of symbols based on its prediction of the next expected packet to be received from a particular IP address. A received packet is rejected if it does not fall within the range and accepted if it is within the range. There is no victim machine of a denial of service of attack and, therefore, no router r or neighbor (n). There is no traceback program. There is no traceback that continues one node upstream of r or “through interconnected routers until a source of denial-of-service attack packets to v is determined or until further traceback is not possible”.

Bhaskaran, which was recited for another reason, does not supply the above noted deficiencies of Munger. Therefore, independent claim 22 is unobvious in view of the combination of Munger and Bhaskaran.

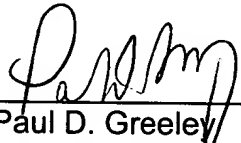
For the reasons set forth above, it is submitted that the rejection of claim 22 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

Newly presented claim 23 is dependent on independent claim 22 and distinguishes from the cited art in the same manner as claim 22. Accordingly, it is submitted that claim 22 distinguishes from the cited art and is, therefore, allowable.

It is respectfully requested for the reasons set forth above that the rejections under 35 U.S.C. 112, 35 U.S.C. 102(b) and 35 U.S.C. 103(a) be withdrawn, that claims 1-23 be allowed and that this application be passed to issue.

Respectfully Submitted,

Date: October 26, 2006



Paul D. Greeley
Reg. No. 31,019
Attorney for Applicant
Ohlandt, Greeley, Ruggiero & Perle, L.L.P.
One Landmark Square, 10th Floor
Stamford, CT 06901-2682
(203) 327-4500